State of Montana Information Security Advisory Council

Council Meeting Minutes
February 18, 2016
1:00 p.m.
DEQ Lee Metcalf Building - Room 111

Members Present:
Lynne Pizzini, SITSD/CISO - Chairperson
David Watterson, City of Kalispell
Joe Chapman, DOJ
Bryan Costigan, MATIC/DOJ
John Daugherty, COR
🖱 Sherri Davidoff, LMG Security
Stuart Fuller, DPHHS
Kreh Germaine, DNRC
James Gietzen, OPI
Adrian, Irish, University of Montana
Margaret Kauska, DOR
Craig Stuart, DMA

Staff Present:
Joe Frohlich
Jennifer Schofield
Tim Wunderwald
Luann Metro

Guests Present:
Carroll Benjamin, Curt Norman, Daniel Nelson, Dawn Temple, Dylan Dickson, Jeff Tschida, John Cross, Manuel Soto, Mike Mazanec, Sarah Norman, Sean Rivera, Suzi Kruger, Tim Kosena.

🖱 **Real-time Communication:**
Angie Riley, Chris Kuntz, Christi Mock, Darrin McLean, Jerry Kozak, Kyle Belcher, Lisa Vasa, Michael Jares, Miranda Keaster, Phillip English, Sky Foster, Terry Meagher.

<u>Welcome and Introductions:</u>
Lynne Pizzini welcomed the council to the February 18, 2016 MT-ISAC meeting. All members and guests were introduced.

Minutes: The January 20, 2016 meeting minutes were approved with no changes.

<u>OPI's Plan for Developing Security within the agency, Curt Norman</u>
Curt Norman the Network Systems Analyst for the Office of Public Instruction gave a presentation OPI's Security Plan. This high level plan was developed for staff to give them an understanding of the importance of security and how OPI complies with federal standards and State of Montana statues and policies. This plan also serves as a roadmap for the agency on how security will be implemented throughout OPI's environment and systems. For further information, please contact Curt at cnorman@mt.gov or (406) 444-3536.

Q: Margaret Kauska verified the timeline of implementation of the plan from January 2016 through January 2020. Margaret asked how many employees were dedicated to the project.

A: Curt Norman answered OPI began with 1.5 FTE and ended with 2.0 FTE.

Q: Jeff Tschida asked why OPI referred to NIST Device Risk Management Framework. NIST is a large organization and he does not understand the terminology.

A: Curt Norman explained that the primary focus with the 18 control families is NIST 800-53. He did not add that information into the presentation (available on the ISAC website) as he did not want to lose focus. However, the information is available in the Information Systems Security Plan (ISSP) (also available on the ISAC website) for anyone interested.

Q: Jeff Tschida asked if OPI has looked at breaking out the organizational requirements in those 18 control families via system requirements. When Jeff's office was looking for actual system engineering parts, they found only 12 of the families actually have embedded system requirements, all the rest are organizational.

A: Curt Norman explained that it was not necessarily in the scope of OPI's plan at this time. OPI will look at this down the road if it affects their system.

Cybersecurity National Action Plan (CNAP), Lynne Pizzini

Lynne Pizzini reviewed key points of President Obama's Cybersecurity National Action Plan (CNAP) and encouraged everyone to review the National Action Plan. The plan includes establishing a Commission on Enhancing National Cybersecurity, made up of top strategic, business and technical thinkers from outside of Government. A new position will be created, Federal Chief Information Security Officer to drive cybersecurity changes across the Government. Fiscal year 2017 Budget includes over $19 billion for cybersecurity which results to a 35 percent increase from FY 2016. Lynne Pizzini is concerned that the plan only addresses Cybersecurity on a Federal level versus how it affects State, local, and tribal governments.

Workgroup Updates:

Assessment Workgroup Update, Lynne Pizzini

Lynne Pizzini requested the council approve the Governor's Cybersecurity Dashboard, which can be found on the ISAC website.

Q: Bryan Costigan asked if there were other States doing similar initiatives and was there any commonality that could be shared.

A: Lynne Pizzini responded that the workgroup did look at Michigan, and yes, commonalities could be shared.

Q: Stuart Fuller suggested submitting previous month's historical content.

A: Lynne Pizzini will present the Governor's Cybersecurity Dashboard to the Governor's office including the previous month's historical content.

Motion: Stuart Fuller moved to approve the Governor's Cybersecurity Dashboard with suggested edits. Bryan Costigan seconded the motion. The motion carried unanimously.

Q: Bryan Costigan asked if adjustments could be made to the Dashboard in the future.

A: Lynne Pizzini responded yes.

Q: Bryan Costigan asked if we should consider giving this information to other elected officials.

A: Lynne Pizzini replied that it is up to MT-ISAC to pass on information to other officials.

Action Item: Lynne Pizzini, with concurrence from MT-ISAC, will send a copy of the Governor's Cybersecurity Dashboard to Major General Matthew Quinn.

National Cyber Security Review (NCSR), Joe Frohlich

Joe Frohlich reviewed the NCSR, which is available on the ISAC website. He explained how MT-ISAC would utilize this tool to provide a State Information Security Assessment to the Governor on a yearly basis, which report where each agency stands.

Q: Bryan Costigan asked how detailed the report was and who has access to the report as it may identify the State's vulnerabilities.

A: Lynne Pizzini assured him that the information is not disclosed to anyone other than the Governor. Agencies have control over their assessment template. The NCSR report is just an overview that does not include specifics.

Lynne Pizzini reported that the Assessment Document should be ready for review in a couple of weeks.

Best Practices Workgroup Update, Lynne Pizzini

Hardening of Devices, Lynne Pizzini

Lynne Pizzini updated the Council on comments received about the Device Hardening Strategy (available on the ISAC website). One comment suggested adding a section to the document regarding the Windows firewall.

Q: Stuart Fuller wanted to know if the group looked at the IRS Schism's for workstation hardening and would this comply.

A: Lynne Pizzini responded that the group did not.

Action Item: Stuart Fuller commented that he is concerned with the IRS audit and asked if someone could look into the IRS Schism's recommendations for compliance. Margaret Kauska will follow up. ****UPDATE****: The IRS schisms are met within the document by stating: "validating against security benchmarks from trusted sources". One of those trusted sources will be the IRS schisms, and Joe Frohlich will notify the tools group of this requirement.

Q: James Gietzen asked if this document would fit into one of the five families.
A: Lynne Pizzini answered yes and it will specify what requirements were met in the policy.

Motion: Lynne Pizzini called for a motion to accept the Hardening of Devices based on the comparison to the IRS Schism's. Margaret Kauska moved to approve the strategy. John Daugherty seconded the motion. The motion carried unanimously.

List of Best Practices, Lynne Pizzini
Lynne Pizzini discussed the workgroup has identified all the best practices from SITSD's policies and placed them in a list, which can be found on the ISAC website.

Action Item: Lynne Pizzini requested all Council members review the Information Security Best Practices List and provide the workgroup feedback. The number of initials after each item determines the order each item will be worked on.

Incident Handling, Lynne Pizzini
Lynne Pizzini discussed the Incident Handling Steps for large and small incidents (both of which are available to view on the ISAC website).
Q: Stuart Fuller asked that a step be added to the Large Incident Handling Steps in regards to reporting to the appropriate entities should an event occur. Examples include, notifying Risk Management Tort Division (RMTD), the Attorney General, etc.
A: Lynne Pizzini agreed completely and will make the appropriate changes.
Q: Stuart Fuller recommended Lynne also add a generic line for a program to review the specific federal requirements or other requirements for notification. For example, DPHHS has several Federal partners with different timeframes for notification of such events.

Action Item: Lynne Pizzini will add reporting to the appropriate entities and federal reporting timeframes to the Large Incident Handling Steps.

Security Policy Template, Lynne Pizzini
Lynne Pizzini discussed the Security Policy Template (which can be found on the ISAC website). Lynne explained the policy could be utilized by agencies that do not currently have an Information Security Policy in place.

Tools Workgroup startup, Lynne Pizzini
Lynne Pizzini discussed the Best Practices Workgroup needs a way to implement the best practices. Therefore, the workgroup would like the Council to approve the Tools Workgroup to be used and to implement the newly approved Device Hardening Strategy. Lynne requested volunteers.

Action Item: Dawn Temple will chair the group. Adrian Irish, Suzi Kruger, Sean Rivera and Mike Mazanec will participate as members.

Lynne Pizzini continued, the assembling of the group would be announced at the next ITMC and NMG meetings to solicit more members. She asked that those members be technical staff who would help decided on the best ways to implement Device Hardening Strategy.

Outreach/Training and Awareness groups, Joe Frohlich
Joe Frohlich discussed the Enterprise Security Program (ESP) and accomplishments over the last few months. One accomplishment includes promoting training and awareness for the Montana school systems. ESP presented at MACO Conference in Great Falls, MT. ESP is happy to announce they were well received.

Joe Frohlich indicated Lynne Pizzini would be speaking at the Montana Educational Technologist Association (META) conference March 19, 2016 in Helena, MT. More information about this conference will be distributed later. ESP will also have a booth at the conference to promote awareness and training.

Joe Frohlich congratulated the winners of the ESP Professional Training Grant. Seven candidates were selected. ESP will be applying for the grant again in spring 2016.

Situational Awareness Workgroup Update, Brian Costigan
Bryan Costigan discussed the Incident Response Document, which can be found on the ISAC website. Brian has been working on what agencies do or do not need to report on the Incident Response Document.

Q: Joe Chapman asked why Cybersecurity was on the document versus Information Security.
A: Bryan Costigan reported that there was no significance in the naming convention.

Action Item: Brian Costigan will have the final Incident Response Document for review at the March MT-ISAC meeting.

Current Threats, Sean Rivera
Sean Rivera presented on current threats. Sean detailed three threats agencies need to be aware of are Smart TV's, MazarBot Malware and Ransomware. Smart TV's are transmitting voice data information back to the companies that own/sell the equipment. MazarBot Malware is obtaining administrative privileges through SMS text messaging. Ransomware locks up a system until a ransom is paid.

Q: Mike Mazanec asked if there are any indication of the attack vector and what it was with ransomware.
A: Lynne Pizzini responded the vector was identified but not what it was.

Sean discussed the SITSD's Disaster Recovery coordination is planned for 2nd week of June. Agencies are welcome to join, please contact Sean Rivera (srivera@mt.gov) or your CRM.

Open Forum
Lynne Pizzini informed the group that MT-ISAC meeting on August 18, 2016 conflicts with TechJunction. There may be a possible agenda item to reschedule the August 18, 2016 meeting.

Public Comment - None

Next Meeting - March 17, 2016, DEQ Lee Metcalf Building, Room 111

Adjourn - The meeting adjourned at 2:32 p.m.

Adopted March 17, 2016